Bachelor's thesis

Information & Communications Technology

2020

Taneli Vuori

WIRELESS COMMUNICATION TECHNOLOGIES AND SECURITY IN 5G

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information & Communications Technology

2020 | 37 pages

Taneli Vuori

WIRELESS COMMUNICATION TECHNOLOGIES AND SECURITY IN 5G

5G is becoming a global phenomenon and it is currently being implemented in a couple dozen countries including Finland. With it comes new information security challenges. The purpose of this work was to get acquainted with wireless communication technologies and the information security challenges they create from the viewpoint of 5G and its preceding technologies. Potential solutions for the challenges are also offered.

This thesis is carried out as a literature review. Books, researches and scientific publications are used as references.

The outcome of this research was an overview of information security challenges in 5G and in the technologies preceding 5G. Possible information security solutions are presented in this work for the new technologies coming with 5G.

This work showed that the new technologies coming with 5G, such as the virtualization of hardware and services as well as the utilization of cloud computing, create completely new areas of attack for networks. With this knowledge, it is possible to prevent attacks targeting networks by implementing necessary information security elements.

KEYWORDS:

5G, wireless communication, security, network, technology

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2020 | 37 sivua

Taneli Vuori

LANGATTOMAT VIESTINTÄTEKNOLOGIAT JA 5G-VERKON TURVALLISUUS

5G:stä on tulossa maailmanlaajuinen ilmiö, jota tällä hetkellä ottavat käyttöön muutamat kymmenet maat Suomi mukaan lukien. Se tuo mukanaan uusia tietoturvallisuushaasteita. Työn tarkoituksena oli perehtyä langattomiin viestintäteknologioihin ja niiden luomiin tietoturvahaasteisiin 5G:n ja sitä edeltävien teknologioiden näkökulmasta. Mahdollisia ratkaisuja näihin tietoturvahaasteisiin on myös esitelty.

Opinnäytetyö toteutettiin kirjallisuuskatsauksena. Lähteinä käytettiin aiheesta tehtyjä kirjoja, tutkimuksia sekä tiedejulkaisuja.

Tutkimuksen tuloksena oli yleiskatsaus 5G:n ja sitä edeltävien teknologioiden tietoturvallisuushaasteista. Mahdollisia ratkaisuja tietoturvahaasteisiin on esitetty tässä työssä 5G:n mukana tuleville uusille teknologioille.

Työssä kävi ilmi, että 5G:n mukana tulevat uudet teknologiat, kuten laitteistojen ja palveluiden virtualisointi sekä pilvipalveluiden hyödyntäminen, luovat täysin uusia hyökkäyspinta-aloja tietoverkkoihin. Tämän tiedon avulla voidaan ennaltaehkäistä tietoverkkoihin kohdistuvia hyökkäyksiä ottamalla käyttöön tarvittavia tietoturvaelementtejä.

ASIASANAT:

5G, langaton viestintä, turvallisuus, tietoverkko, teknologia

CONTENTS

PICTURES

LIST OF ABBREVIATIONS

0G	Pre-cell era
1G	First Generation of wireless cellular technology
2G	Second Generation of wireless cellular technology
3G	Third Generation of wireless cellular technology
4G	Fourth Generation of wireless cellular technology
5G	Fifth Generation of wireless cellular technology
3GPP	3rd Generation Partnership Project
AKA	Authentication and Key Agreement
AMPS	Advanced Mobile Phone System
API	Application Programming Interface
CDMA	Code-Division Multiple Access
CSP	Communication Service Provider
D2D	Device to Device
DoS	Denial of Service
EAP	Enhanced Authentication Protocol
eMBB	enchanced Mobile Broadband
ETSI	European Telecommunications Standards Institute
GSM	Global System of Mobile Communications
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity

IoT	Internet of Things
IS-95	Interim Standard 95
ITU	International Telecommunications Union
LTE	Long Term Evolution
M2M	Machine to Machine
MAC	Medium Access Control
MANO	Management and Orchestration
MCC	Mobile Cloud Computing
MEC	Mobile Edge Computing
MIMO	Multiple-Input Multiple-Output
MMS	Multimedia Messaging Service
mMTC	massive Machine Type Communications
mmWave	millimeter Wave
NAS	Non Access Stratum
NFV	Network Function Virtualization
NGMN	Next Generation Mobile Networks
RAN	Radio Access Network
RRH	Remote Radio Heads
RSA	Rivest-Shamir-Adleman
SDN	Software Defined Networking
SIM	Subscriber Identity Module
SMS	Short Messaging Service
SS7	Signalling System No. 7

TACS	Total Access Communication System
TMSI	Temporary Mobile Subscriber Identity
UE	User Equipment
UIM	User Identity Module
UMTS	Universal Mobile Telecommunications Service
uRLLC	ultra Reliable Low Latency Communications
VMNO	Virtual Mobile Network Operator
VM	Virtual Machine
VNF	Virtual Network Function
WiMAX	Worldwide interoperability for Microwave Access

1 INTRODUCTION

5G technology has arrived upon us and it is starting to spread across the globe. The technology is here, and it will have information security implications.

This thesis addresses the security problems that 5G has or might have in the future. This is a concern that will touch quite literally everyone who has or will have a 5G connection on their mobile phones, computers or other devices. It is a major concern in terms of Internet of Things (IoT) as well. Now is a good time to talk about this, for we are at the beginning of an 5G era. This era may last for quite a while, and 5G will most likely be the dominating wireless connection technology. This thesis also discusses technologies before 5G, and their security features and vulnerabilities.

Since 5G is rather new technology, most of the information regarding 5G is from internet sources with some book sources used as well. One of the most used references in this thesis is the book *A Comprehensive Guide to 5G security* [1] as it is one of the few thorough books produced of this subject.

The goal of this thesis is to go into the world of information security and try to give a good level of understanding about the new technologies affecting 5G security to anyone who reads this thesis. The thesis is divided into 7 chapters, 1st chapter being this introduction. The 2nd chapter of this thesis goes over the previous technologies with their security challenges and solutions. In this part the history of the technologies and when they were first introduced is discussed. The 2nd chapter starts with the pre-cell era, and goes through both 1G and 2G, as they are older technologies. In chapters 3 and 4 the wireless communication technologies of 3G and 4G are introduced, as they are widely in use. Chapter 5 presents the 5G enabling technologies and chapter 6 introduces the different security methods used in the new technologies coming with 5G and their solutions, as well as challenges in privacy. 7th chapter concludes the research into a comprehensive chapter where the findings of the new technologies coming with 5G are recapped. In the final chapter the future of 5G and its security is also discussed.

2 EARLY IMPLEMENTATIONS OF MOBILE TECHNOLOGIES AND THEIR SECURITY FEATURES

5G is the fifth generation of wireless communication technology. To recap how the technology has developed in past years, this chapter will take a short look of the previous technologies that preceded 5G, namely 0G, 1G, 2G, 3G and 4G. This is done so we can build an understanding of what was, and why 5G is what it is today.

2.1 Pre-cell era

0G, also called pre-cell era, became available after the second World War. Mobile operators would have to connect the calls manually, and there were only few channels available at once. Mobile radio telephonic systems were the predecessors of first generation of cellular telephones, and two of the technologies that were used were mobile telephone service and improved mobile telephone service. The two analog technologies mentioned were direct continuations of each other and were developed for 20 years from early 1960s to early 1980s. [2]

2.2 First generation of wireless cellular technology

Introduced first in 1979 to the world in Tokyo, Japan, 1G brought with it the first generation of wireless technology and analog cell phones. Two of most-used technologies were Total Access Communication System (TACS) and Advanced Mobile Phone System (AMPS). These systems provided handover and roaming capability but were unable to operate between different countries. 1G was extremely susceptible to eavesdropping, as it only required a receiver that operated on similar frequencies to listen in on the calls, so 1G had zero confidentiality in communication. [1,2]

2.3 Second generation of wireless cellular technology

The first version of Global System for Mobile communications (GSM) was released in 1990, and it was first deployed in Finland in July 1991. The overall performance of the

system improved drastically when modulation schemes were changed from analog to digital. 2G cellular systems comprise of Digital-AMPS, Code-Division Multiple Access (CDMA), personal digital communication and GSM. GSM is the most widely used and successful 2G cellular network system, and targeted spectrum efficiency, international roaming, better voice quality, compatibility, ability to support new services and low mobile and base stations cost. 2G and GMS were very popular with users because of Short Messaging Service (SMS) and Multimedia Messaging Service (MMS), which enabled users to communicate more effectively among each other. The MMS especially was very popular with the users. Data speeds with GSM were up to 14.4 Kbps using circuit switched data. GSM technology serves as the base for next generation, 3G, systems and Long Term Evolution (LTE). There is also a standard called Interim Standard 95 (IS-95), also called cdmaOne. IS-95 is the base for future CDMA 2000 technology, but since IS-95 is not so widespread, this chapter will focus solely on GSM. [1,2]

2.3.1 GSM security

Since GSM was the most used standard and remains to still be used to this day, though several countries have already began to phase out 2G [3], it is good to know more about this standard, as it is the base for future technologies.

GSM is the first to use actual security methods, such as authentication, confidentiality of user identity, ciphering of data and the usage of Subscriber Identity Module (SIM). SIM is used to store subscriber information, which in turn is used to prove the identity of the device owner and the services the user is allowed to access. Authentication requires the user to confirm to the operator that they are a credible customer requesting the service. Ciphering is used to send data and signals in such a way, that hijacking any information would not be possible. GSM uses Temporary Mobile Subscriber Identity (TMSI), that is derived from International Mobile Subscriber Identity (IMSI), to grant users confidentiality. IMSI provides every subscriber in the world an unique number, up to 15 digits, that carries the information of their home network and country it belongs to. IMSI is usually not sent to the operators when authenticating due to possible eavesdropping, instead TMSI is used, as it is a temporary number and that way of no use to outsiders. GSM also uses symmetric algorithms A3 and A8 between the GSM operator and the user, which means there is a single key that is used to encrypt and decrypt data. This

key is generated in the SIM. The algorithms have a one-way behavior, which means that the output can be found if the inputs are known, but not vice versa. [1]

2.3.2 GSM vulnerabilities

Although GSM is being replaced by Universal Mobile Telecommunications Service (UMTS) and LTE, it still offers the highest coverage, and in some places, users do not even have an alternative to choose from. This exposes many of the users to threats that arise from using an outdated standard. The openness of wireless communications makes the users communicating more vulnerable to security threats. GSM tried to harden the interception using several different techniques, such as frequency hopping, but it is still completely vulnerable to multiple different attacks targeting a part of the network. To list a few, GSM has vulnerabilities concerning man-in-the-middle attacks using a false base station, flaws in implementation of A3/A8 algorithm, SIM card cloning, over-the-air cracking and short range of protection. [4,5]

Much has been done to combat vulnerabilities and GSM has had its gradual improvements during the years, that have led to versions such as GSM1800, high speed circuit switched data, enhanced data rates for GSM evolution and general packet radio service. The GSM improvements are continued in 3G systems, such as UMTS. Some solutions to the GSM security flaws include using secure algorithms for A3/A8 implementations. This can prevent SIM card cloning attacks, and therefore securing the backbone traffic and implementing end-to-end security to the application layer. [5]

3 THIRD GENERATION OF WIRELESS CELLULAR TECHNOLOGY

The planning of 3G systems was started in the early 1990s, and it was mainly developed by International Telecommunications Union (ITU), who proposed multiple things that are collectively known as IMT-2000. The objective was to implement blueprints for global harmony for mobile communication, which would be able to commence global interoperability by providing reduced cost. ITU set the requirements for data rates of 3G as follows: 2 Mbps in building or fixed environment, 384 Kbps for urban environments and 144 Kbps for vehicular wide area environments. Compared to 2G, the speeds really skyrocketed, and apart from the above requirements, the 3G systems were also intended to bring better quality of service across the board. [1]

The two systems that were first introduced were UMTS and CDMA 2000. Both technologies comply with the speed requirements introduced by ITU. In 1998 a joint collaboration was formed and named 3rd Generation Partnership Project (3GPP), that serves as an umbrella for a number of standards, such as GSM, UMTS, LTE and 5G new rad. [6] The purpose of 3GPP originally was to develop UMTS along with other GSM standards. The first UMTS standards were published in 1999. The responsible for official standardization process of CDMA 2000 was a standard committee named 3GPP2. CDMA 2000 is a continuation for IS-95. [1] All of the 3G technologies are still widely used to this day.

3.1 CDMA 2000 security

There are a total of four entities engaging in the CDMA 2000 security architecture, and those include the home network with its home location register and authentication center, the serving network with its location register and mobile station controller, the mobile station and the User Identity Module (UIM), such as IMSI. CDMA 2000 uses similar Authentication and Key Agreement (AKA) as UMTS, so it achieves mutual authentication by the user and the network. Both of those participants share the knowledge of a secret key, which is only available to those two. This subscriber key is either manually put in to the UIM or it is made with over-the-air service provisioning by calling a service number. The AKA is implemented in two stages. At the first stage the security credentials are

passed from the home network to the serving network. In the second stage a one-pass challenge-response procedure is made to achieve mutual authentication between the UIM and the network. [7]

3.2 UMTS security

As previously mentioned, UMTS is the continuation of GSM technology, so its security solutions are similar as well. UMTS security architecture is divided to five different sets of features. Network access security gives users secure access to the 3G servers and protects against possible attacks to the radio interface. Network domain security makes the signaling of data secure and it also brings protection against attacks aimed at the wireline network. User domain security handles the safe access to mobile stations. Application domain security verifies that the applications in both the user and provider domain can communicate with each other in confidence. Visibility and configurability of security gives security information to the users, and guidance regarding whether a certain security feature requires switching on. UMTS AKA is used in UMTS as well as in CDMA 2000. [1]

3.3 3G vulnerabilities and Signalling System No. 7

Vulnerabilities in newer technologies are becoming harder to find as network providers tend to not announce any flaws they might have in their systems, unless confronted, as it would compromise the security of the systems themselves. Since 3G technologies are still widely in use, making security flaws public knowledge is something that people should be careful with. However, as some of the vulnerabilities are already widely known and exploited, talking about them raises awareness and pressures network providers and even protocol developers, such as 3GPP and 3GPP2, to increase their security standards, whether by phasing out older standards such as 2G and 3G in areas where they are not needed or increasing the security mechanisms in those technologies. As going over every single vulnerability there is would take hundreds of pages of text, only the most prevalent ones are discussed.

An underlying problem in 3G systems, UMTS and CDMA 2000, is the Signalling System No. 7 (SS7). SS7 is a set of protocols that are in charge of exchanging signaling messages in 3G systems. It was developed in 1975, when there was no wireless access

to networks and the security risks were less relevant than what they are today. SS7 has hardly been updated since then. This outdated standard is vulnerable to interception of SMS messages and calls, subscriber Denial of Service (DoS) and information disclosure attacks. SS7 has already been exploited by criminal entities, for example in Germany, bank accounts have been compromised by exploiting the two-factor authentication system used by German banks, which sends a code to a mobile phone before funds get transferred between accounts. [8] Network operators are aware of the problems caused by SS7 but are sometimes inadequately prepared to do anything about it. According to Positive Technologies network security analysis [9], only 30 percent of European telecom operators have implemented the GSM associations security recommendations. Solutions to these problems caused by SS7 seem to mainly be moving towards newer technologies in 4G and 5G, or actively monitoring and analyzing signaling traffic that crosses network boundaries to catch potential threats early. This implementation of monitoring is also included in the GSM associations recommendations.

4 FOURTH GENERATION OF WIRELESS CELLULAR TECHNOLOGY

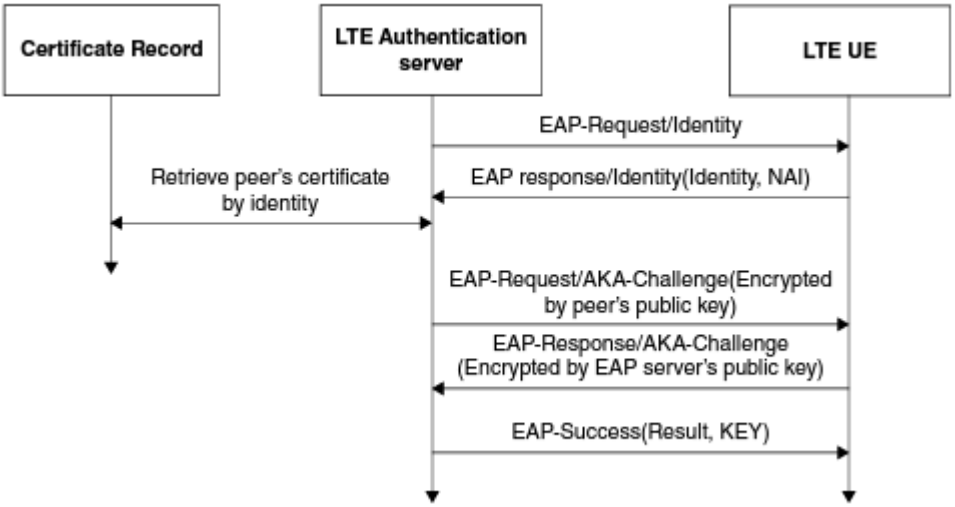
The first commercial release of 4G LTE was at the end of 2009 in Stockholm. [10] For a system to be called 4G, they must meet the criteria assigned by ITU. This criterion is called IMT-Advanced. The requirements include network speed qualifications, 100 Mbps for high mobility and 1 Gbps for low mobility, worldwide roaming capability and mobile devices with high quality, among other things. Performance requirements are a bit more diverse than this, and they are specified in the IMT-Advanced to the fullest. [1]

The two 4G technologies are called LTE and Worldwide interoperability for Microwave Access (WiMAX). They both operate entirely on IP protocol and architecture, which makes them rather similar in how they work. They do differ from each other in security solutions. IP-based infrastructure brings with it a lot of potential security issues, so extra work must be put into the security mechanisms in both of these technologies to provide a secure and reliable communication line. LTE is backed up by 3GPP, whereas WiMAX is based on the 802.16 wireless broadband standards written by the Institute of Electrical and Electronics Engineers (IEEE). [1] The two technologies were competitors, but in the end LTE took the title of dominating the area 4G, making WiMAX an obsolete technology. [11]

There are many technologies that make 4G possible. Multiple-Input Multiple-Output (MIMO) is a key technology in the current 4G and 5G systems. It introduces the use of multiple antennas in both the transmitter and the receiver side. 4G also introduces the use of carrier aggregation and relays. Carrier aggregation means the use of multiple carriers simultaneously so that devices can use greater amount of data. A singular carrier provides 20 MHz bandwidth in LTE. Relays receive, demodulate and decode the data, apply any error corrections, then re-transmits a new signal so that the signal quality is enhanced. [12] The purpose of relays is to provide coverage in new areas, make temporary network areas and also to offer high data rave coverage and group mobility. [1] There are many other technologies that will be mentioned further down in the actual 5G section, and the technologies mentioned will be expanded in there.

4.1 LTE security

In the book *A Comprehensive Guide to 5G Security*, an excellent step-by-step picture of LTE authentication is provided. This picture is used to illustrate the authentication process in LTE, since explaining the method by just using words would be insufficient and confusing. In Picture 1 on the right side there is the User Equipment (UE), in the middle the authentication server, which starts the authentication process by sending an Enhanced Authentication Protocol (EAP) request, and on the left the certificate record, which generates the AKA-challenge message and sends it to the authentication server that sends it to the user. The picture is read top-down.



Picture 1. Authentication Process in LTE [1].

The second part of LTE security is Non Access Stratum (NAS). It is designed to establish a secure connection between the UE and the mobile management entity across radio links. It also performs integrity checks and ciphering of the NAS messages. Different keys are used in order to perform integrity checks and ciphering. NAS keys are derived by UEs and mobile management entities. [13]

The third part is the access stratum security. Its purpose is to safely deliver data between an UE and nodes. It performs integrity and ciphering checks of signaling messages in the control plane. Once again, different keys are used in order to perform integrity checks and ciphering of signaling messages and IP packets. [13]

4.2 WiMAX security

WiMAX is not really used to this day anymore. However, it uses the 802.16 family of standards. The IEEE 802.16 protocol architecture consists of two main layers, the Medium Access Control (MAC) and the physical layer. MAC layer features 3 sub-layers, which are service specific convergence sublayer, MAC common part sublayer and security sublayer. The point of focus here is the security layer, which is in charge of key establishment and exchange, encryption and decryption as well as authentication. The security layer acts as an intermediary in between the MAC and physical layer, being in charge of the data exchanged. [14]

In the security layer there are three WiMAX security features that are mentioned that protect the base station and UE. First of them is called security association, which is a set of security information parameters that the base station and UEs share. The security association contains a cryptographic identifier, initialization vectors and traffic encryption keys. Second security feature is the public key infrastructure. WiMAX uses privacy and key management protocol for key management, exchange and transfer among the mobile stations. It uses advanced encryption standard as its encryption algorithm. Third in the list is user authentication. It features three different types of authentications, where the first one is Rivest-Shamir-Adleman (RSA) based authentication. EAP based authentication is the second method, which is similar to the LTE authentication process. Third authentication type is a combination of the two previously mentioned, RSA and EAP. [14]

4.3 4G vulnerability examples

Whereas GSM networks were vulnerable to rogue base stations, LTE is assumed to offer confidentiality in that regard. However, LTE networks are vulnerable to threats that target privacy, authentication and availability. Although LTE does provide mutual authentication and strong encryption, it is sometimes wrongly assumed to be enough. LTE is still vulnerable to great deal of threats, such as location leaks, rogue base stations and protocol exploits. Despite the mutual authentication and strong encryption, a large portion of the control plane signaling messages are exchanged over the LTE radio link in clear sight. Before all the encryption and authentication steps can take place, a mobile device will start communicating with a LTE base station that advertises itself as a legit

base station, whether it is legit or not, leading to the users identity being compromised if it is indeed a rogue base station. This communication between the device and base station is vulnerable to sniffing. This type of an attack is also called an IMSI attack, and it continues to be a problem in 5G as well. [15]

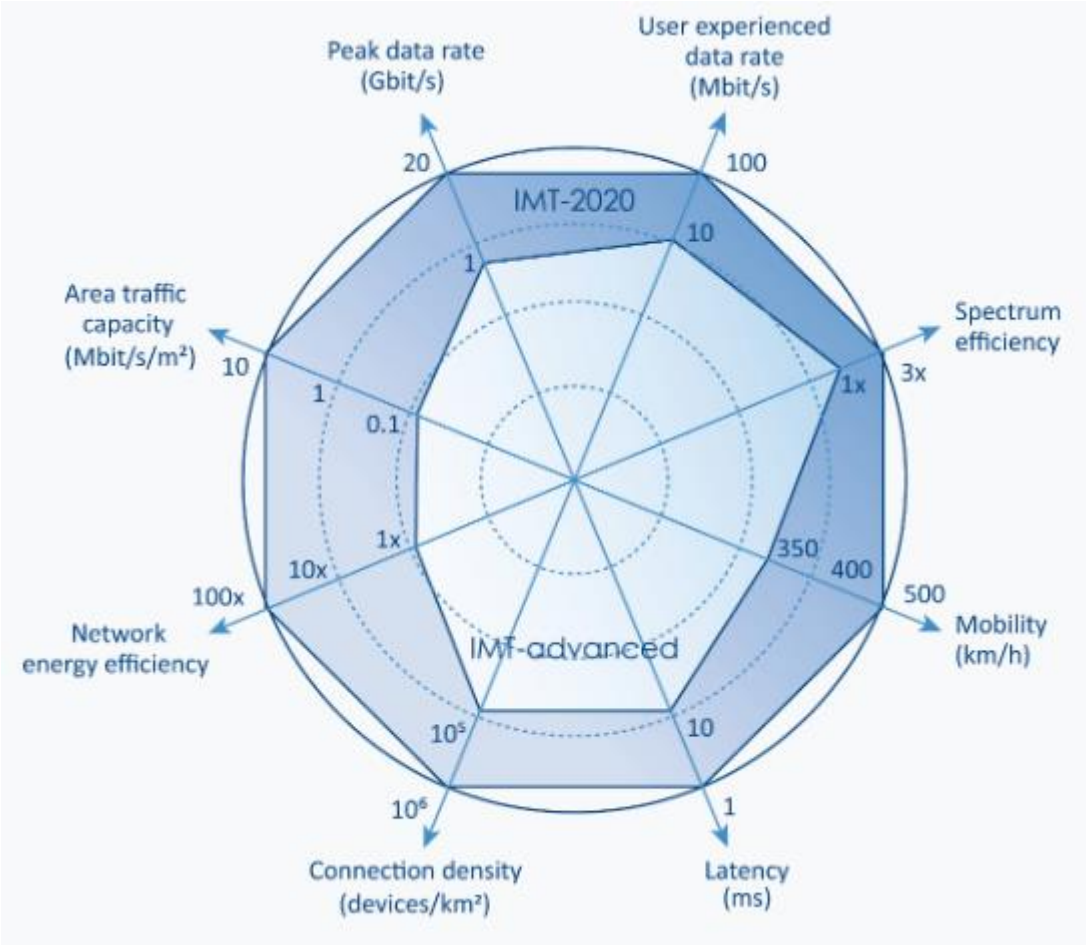
Another commonly known threat is the downgrading to a GSM connection. This attack exploits the *Attach Reject* and *Attack Request* messages, that allow the base station to block certain mobile devices if they engage in malicious behavior. However, this enables rogue base stations to use these messages as well, and this way they can disallow the device to connect to LTE services. This makes the device only attempt to connect to GSM base stations, which are less secure. This attack can also be done together with a GSM rogue base station, so that the attacker would be in complete control of the networks the user uses, and in this way enabling the possibility for eavesdropping everything that the user does, such as phone calls and text messages. These *Attach Reject* and *Attack Request* can also be used just to block users from accessing the network completely. [15]

5 FIFTH GENERATION OF WIRELESS CELLULAR TECHNOLOGY

1G brought analog mobile voice calls. 2G added digital voice calls and SMS to that. 3G introduced mobile web browsing. 4G revolutionized the data speeds and brought mobile video consumption to all its users. The traffic of mobile data grows larger by the day, and 4G alone is probably not going to be enough. Ericsson predicts that in 2023 there will be 9 billion mobile subscriptions and 20 billion connected IoT devices. [16] In 2019 the number for global mobile subscriptions was approximately 5,2 billion and the amount of IoT devices was estimated to be 12 billion. [17] The presumed huge increase in these numbers is obviously going to generate more mobile data traffic, which demands more from the mobile network operators and from the technologies they use. As more devices get connected to the internet, security measures must be actively sought out and implemented. Next, the 5G enabling technologies are presented before moving on to the security aspects of 5G.

5.1 5G enabling technologies

There are certain requirements that must be met with the implementation of 5G. To list them, they are high data rate, ultra-low latency, massive connectivity, reliability and high availability, flexibility and programmability, energy and cost efficiency, spectrum efficiency, security and privacy. The development and implementation of different technology candidates happens in the Radio Access Network (RAN), the core network and in the end-to-end system. Many different standardization organizations, such as ITU, 3GPP, IEEE, European Telecommunications Standards Institute (ETSI) and Internet Engineering Task Force (IETF) are researching these different technologies and providing standards on which to base the systems to. Especially ITU continues its leading role in outlining the vision for 5G. ITU controls the IMT-2020 standard, which contains the requirements for 5G networks. [1] Picture 2 (reference) below compares the IMT-Advanced, which includes the requirements for 4G LTE, and IMT-2020. It compares the key capabilities of both the requirement standards. We can see, that for example the area traffic capacity and network energy efficiency are predicted to increase hundredfold.



Picture 2. Comparison of capabilities between IMT-Advanced and IMT-2020 [18].

5.1.1 Radio Access Network

There are six enabling technologies for 5G RAN. First off, we have millimeter Wave (mmWave), which is a key feature in the 5G system. As 5G is going to have higher capacity in data rates, it requires more spectrum. Current systems are normally operating in the spectrum bands between 700 MHz and 3 GHz. This spectrum range is not sufficient for 5G, so the solution for this is to use higher bandwidth ranges, from 24 GHz to 100 GHz. This section of the spectrum is rarely used, so 5G has an open track ahead of it. The wavelengths of mmWave is between one and ten millimeters, so its penetration capabilities are quite weak. However, solutions to this have already been made, such as beamforming and massive MIMO, which are discussed in the following chapters. [1]

Massive MIMO is a solution for the requirements of 5G when talking about network density and capacity enhancement. Basically, the solution is to deploy more antennas. Normal MIMO has already been utilized in 4G networks, where users are simultaneously

served by multiple antennas at once to enhance the signal. The change to 5G is the number of antennas used, that is that makes it massive. Beamforming is a technology which is part of massive MIMO. It means that the same signal is sent from multiple antennas at once, so the receiver will receive multiple copies of the same signal. This technology allows the signals to constructively sum up, which makes the signal stronger. This technology is also said to enhance energy efficiency, which obviously interests the network operators installing these required new antennas. [1]

The third feature of RAN is called ultra-dense small cells technology. The purpose of these small cells is to bring the network closer to the users, making it easier to have good service in high traffic and hotspot areas. These small cells have a lot shorter coverage range, from couple tens of meters to couple hundred meters. This means there must be a lot of them, which poses challenges in terms of management and interference. [1]

Fourth feature is Machine to Machine (M2M) and Device to Device (D2D) technologies. As mentioned previously, approximately two-thirds of all 5G related communication is going to happen M2M. M2M communication was already a thing in 4G LTE systems and continues to be that in 5G. M2M communication refers to the automated communication between machines. This communication method enables a number of different services, such as monitoring, automation, health care and automotive. M2M does have some challenges with security and privacy, as most of the time the machines spend their time unattended, which makes physical attacks possible. The machines usually also possess rather low capabilities in terms of energy and computing resources, and therefore they cannot implement complex security measures. D2D communication means a direct communication between two mobile devices, without going through a network framework. This means that the network framework in question has basically more capability to handle other requests, as it offloads some of the traffic to D2D communication. D2D offers improvements across the board, such as spectrum efficiency and user data rate gain. It is used in gaming, vehicular communications and proximity-based applications, but also suffers from security problems. [1]

Cloud-based RAN is the next technology. It offers a design for the radio access part of 5G networks with reduced cost and energy efficiency. Cloud-RAN also provides better network speeds and capacities. The technology connects Remote Radio Heads (RRH) with high speed fibers to the baseband unit pool, which generates and processes a digitized radio frequency signal. This technology allows for flexibility, but has drawbacks, such as problems in placing the RRHs. [1]

Mobile Edge Computing (MEC) and its sibling fog computing are technologies that try to bring the services and processing capabilities to the perimeters of mobile networks, so it is as close to the end users as possible. The purpose of this is reduce latency as much as possible and produce an efficient network. For example, IoT, augmented reality and connected cars all require very low latencies, which MEC can provide. Fog computing is basically the same, but for cloud computing resources. Those resources are extended to the boundaries of the network, in order to achieve similar results as with MEC. [1]

5.1.2 Mobile Core Network

Software Defined Networking (SDN) is a rather new term, as its only been around beyond academia for a decade. [19] The idea is the physical separation of the data plane from the control plane, so the application layer, control layer and infrastructure layer are isolated. This allows for flexible and programmable network infrastructure, which in turn helps mobile operators bring new services and innovations as fast as possible to the end users. [1]

Network Function Virtualizaton (NFV) introduces the ability to relocate network functions from costly hardware to cheaper software. This allows for virtualization of network devices. One of the reasons this technology exists is the massive reduction in cost, which impacts the revenue of mobile operators, so obviously they have an interest in this. NFV does also provide dynamic scaling of resources and faster deployment of new services. [1] SDN and NFV have some similarities in terms of virtualization and can be used together to further develop networking technologies, such as network slicing, which is discussed in the end-to-end system chapter.

5.1.3 End-to-End system

There are few key technologies for constructing an end-to-end system, and the first of them is network slicing. As 5G is expected to support different types of services and applications, slicing the network in sections can provide different features and network capabilities to different slices. These slices can have differences in data rates, mobility, reliability, latency and security. Each slice would be an end-to-end isolated system, which makes this a foundation to build 5G on. Network slices are expected to be logically isolated networks, so they could be programmed separately. Example use cases of

network slicing would be slices for enhanced Mobile Broadband (eMBB), ultra Reliable Low Latency Communications (uRLLC) and massive Machine Type Communications (mMTC). Basically, eMBB is for end users, uRLLC for autonomous cars and others that require low latency and mMTC for IoT. [1]

5G is gaining more and more traction by the day, as in 2020 there are already multiple locations that have 5G connectivity available. For example, Finnish telecommunications company Elisa Oyj has already implemented 5G in couple of cities in Finland, such as Tampere, Helsinki and Turku. [20] With this being the case, Management and Orchestration (MANO) of the networks becomes relevant. MANO has already been in use in 4G networks and will be or is already in use in 5G networks. The role of MANO is managing all the network infrastructure in terms of security, performance, accounting, configuration and fault management. It is also in charge of network provisioning for the network slices in order to provide end-to-end connectivity. Current system used in 4G needs to be expanded in order for it to be sufficient for the 5G networks. [1]

6 5G SECURITY CHALLENGES AND POSSIBLE SOLUTIONS

As the 5G network security is a large subject, the focus will be on the new technologies coming with 5G. Among the new technologies are terms such as SDN, NFV and mobile cloud, which are discussed in the previous chapters, and which will be opened a bit more in the following chapters. Privacy aspect of 5G is also discussed, as it is an interesting subject for the customers.

6.1 New technologies: SDN, NFV and cloud systems

Next Generation Mobile Networks (NGMN) is a mobile telecommunications association of research institutes, manufacturers, vendors and mobile operators, that was founded in 2006 to evaluate wireless network technologies candidates and develop common solutions for them. NGMNs objective is to assure a successful commercial launch of the mobile broadband networks with means like roadmaps and user trials. Its objective is also to support the standards organizations such as 3GPP and IEEE to help them understand what mobile operators need. NGMN has listed challenges for 5G in its white paper [21] that was released in 2015, and there it specifies SDN, NFV and mobile cloud to be technologies, that solve some of the upcoming or ongoing problems, such as network flexibility and virtualization of the mobile core network.

Picture 3 (reference) overviews the 5G security threats with SDN, NFV and cloud systems in mind. It also includes columns links and privacy, where the former considers the links in between networks and the latter is about users' privacy challenges. As we can see from this picture, there are a quite few of these, and some of the possible security threats are discussed in the upcoming chapters as examples.

Security Threat	Target Point/Network Element	Effected Technology			Links	Privacy
		SDN	NFV	Cloud		
DoS attack	Centralized control elements	✓	✓	✓		
Hijacking attacks	SDN controller, hypervisor	✓	✓			
Signaling storms	5G core network elements			✓	✓	
Resource (slice) theft	Hypervisor, shared cloud resources		✓	✓		
Configuration attacks	SDN (virtual) switches, routers	✓	✓			
Saturation attacks	SDN controller and switches	✓				
Penetration attacks	Virtual resources, clouds	✓		✓		
User identity theft	User information data bases			✓		✓
TCP level attacks	SDN controller-switch communication	✓			✓	
Man-in-the-middle attack	SDN controller-communication	✓			✓	✓
Reset and IP spoofing	Control channels				✓	
Scanning attacks	Open air interfaces				✓	✓
Security keys exposure	Unencrypted channels				✓	
Semantic information attacks	Subscriber location				✓	✓
Timing attacks	Subscriber location			✓		✓
Boundary attacks	Subscriber location					✓
IMSI catching attacks	Subscriber identity				✓	✓

Picture 3. 5G technology's security challenges. [22]

6.1.1 Challenges and potential solutions in SDN

As previously discussed in chapter 5.1.2, SDN is a new technology that enables programmability and logical centralizing of the network control planes and enables the support for virtualization. SDN separates the data and control plane from each other. Although these technologies are key elements for 5G's development, they do pose some security challenges with them. Network control centralization can make the controller a bottleneck for the entire network, making it an attack vector in terms of saturation attacks, such as DoS. Enabling programmability means that almost all the network functions can be carried out as SDN applications. With this being the case, there is a possibility that malicious applications are granted access or that Application Programming Interfaces (APIs) are exposed to unplanned software. If the API is exposed, it compromises the network function.

One example of an attack is DoS attack. DoS attacks are a well-known attack type and it also is possible attack angle to SDN. DoS threats can occur in both the control and data plane. In the data plane DoS can be caused by attackers flooding the network elements of the SDN architecture. Most often the attack originates from compromised systems, often called botnets, which are basically a string of connected computers coordinated together to perform a task. These botnets are assigned to flood the targeted SDN with traffic, making the service slow down or halt completely. DoS can be produced at the control plane by congesting controllers through a big number of forged flow arrivals, causing the degradation and interruption of the network. [23]

There are options to deal with DoS attacks. Quick threat identification is essential in shutting down DoS attacks as fast as possible, and SDN provides this with one of features, which is packet level granulation. This provides transparency in a way that you are able to see the packet source, the route the packet takes and the content of the packet. These can be gathered from any network perimeter in SDN systems, whereas normally you would only gather these in the network entry points. Of course, the identification of DoS attack packets is still a problem, but as they get identified early on, a rapid response enables the system to route the traffic to intrusion detection system or to firewalls. [22]

6.1.2 Challenges and potential solutions in NFV

As talked previously, NFV is a technology that enabled virtualizing of network services, such as routers, firewalls and load balancers, which have traditionally run on proprietary hardware. With NFV the need for dedicated hardware for all the network functions ceases to exist, as the services are packaged as Virtual Machines (VMs) on commodity hardware. Although a great advancement in technology, this virtualization does open new threats in terms of security. [1] To avoid confusion, both NFV and Virtual Network Functions (VNFs) are mentioned in the upcoming paragraphs. NFV is the framework, that orchestrates and automates the VNFs. VNF is a single network function in a software form, such as router, firewall or load-balancer. VNFs are deployed as VMs.

One of the security vulnerabilities with NFV is the dynamic nature of VNFs. This can lead to configuration errors and therefore security vulnerabilities. VNFs are also vulnerable to typical cyber-attacks, with example being DoS, sniffing and spoofing. With the virtualization comes also specific threats to NFV that are only applicable to virtualized environment. Some of these are flooding attacks, which fills the hosts memory by initiating incomplete packet connection requests, hypervisor hijacking, in which the attacker aims to take control over the hypervisor who is in charge of the virtual environment within a VM, and VM migration attacks, which aim to exploit VM images as they are moved between physical machines in the network. There can also be private deployments of this technology, where all remote access is prevented. In these cases, NFV is only vulnerable to malicious insiders, such as malicious administrators. [22]

Another challenge is the trust factor in maintenance. The installation and configuration of the physical network devices is often handled by a trusted employee, and there is a

certain level of trust to the device, as it is bought from a retailer and it is tangible. However, as VNFs fetch the needed maintenance dynamically from the cloud, there must be some level of trust between the one who owns the VNF and the one that provides the maintenance to prevent any malicious VNFs from entering the system. [22]

There are almost always as many solutions as there are challenges. In NFV systems, basic solutions to external threats are to use well configured firewall and intrusion detection systems. For internal threats, there are mitigation tools such as role-based access control, that defines the privileges for each role. Preventing infrastructural level attacks can be done with continuous monitoring of network resource consumption levels for each user and blocking malicious requests with a blacklist of IP addresses. Outsourcing sensitive information to external networks can be used in NFV to protect the information and validate data integrity. Cryptographic solutions, for example message stream encryption, can be utilized to assure the confidentiality of VNFs, which in turn makes the whole system that much easier to trust. Trust relationships are essential in increasing the trust among different entities in the NFV environment over its whole life cycle. [22]

Although DoS is a big threat for NFV systems as well, a different example is used here. Misuse of resources, also titled resource theft in Picture 3, is a problem caused by the fact that not all the computing resources necessarily support the multi-tenancy requirements that the NFV users require. This can cause data leakage, abnormal activity and unavailability of the service. Another set of problems comes from the fact that hypervisor is in charge of the isolation and communications of the different entities that generate the VNFs. If hypervisor lacks security, there is a possibility that an attacker could alter the hypervisor to give the attacker extra resources. If the hypervisor fails to isolate users, an user X, attacker, could potentially send intensive traffic to user Y, making the user Y stop accessing the service, and thus freeing up the resources for user X. This is what is called a resource freeing attack, and the consequences can be bottlenecks in the resources, latency of service or even blocking the service completely. [24]

A very simple solution for the resource theft attack is to have a hypervisor scheduler that offers share allocations among the processes, which limits the maximum amount of data a user can have for each virtual service. This makes a single user unavailable to exploit any type of misusing of resources. However, this solution affects the performance of the service. [24]

6.1.3 Challenges and potential solutions in mobile cloud systems and MEC

As the cloud computing systems include diverse resources that are shared among the users, there exists a possibility for a user to spread malicious traffic to affect the performance of the system, access resources of other users or consume more resources. Also, conflicts in network configurations can happen in multi-tenant cloud networks where the users have their own control logic. Mobile Cloud Computing (MCC) is an approach that migrates the core concepts of cloud computing in to the 5G systems. The architectural and infrastructural modifications that are made in 5G do pose challenges in terms of security, as the mobile clouds need to change in order to perform in the 5G systems. The openness and versatility of MCC can backfire, as more vulnerabilities are created, and privacy of mobile clouds can be compromised. [25]

For the MCC systems, the threats can be categorized in to three different sections, namely front-end, back-end and network-based threats. The front-end consists of user platform which includes the mobile terminal on which the applications and interfaces are run in order to gain access to the cloud facilities. The threats to front-end cloud segment can be either physical or application based. Physical threats include the compromising of the actual mobile device or other integrated hardware components. Application based threats consist of spyware, malware or some other malicious software, that are used in order to gain information from the users or disrupt the service the application provides. The back-end part of the MCC is a collection of data storage systems, cloud servers, VMs, hypervisor and protocols that are needed to offer cloud services. Security threats mainly affect mobile cloud servers. Examples of threats to back-end are XML DoS and data replication to HTTP. Network-based mobile security threats target the radio access technologies that connect the mobile devices to the cloud. These technologies include the older ones, such as 4G LTE and Wi-Fi, or the newer ones coming with 5G. There are several attacks threatening this area, such as DoS, session hijacking or Wi-Fi sniffing. [25]

MEC is still in its infancy and there exists a lot of different MEC technologies. This combination leads to the existence of potential malicious activity and privacy issues. Extending the cloud computing capabilities to the outskirts of the mobile networks is what MEC does. The amount of protection that can be provided to the edge hosts is not on par with traditional data centers, where all the machines and systems are centralized. The two biggest security concerns for MEC is the IoT environment enabled by the cloud

systems and the open APIs from where all the content is brought to MEC end users and applications. The implementation of open APIs may create security vulnerabilities in the form of man-in-the-middle attack, DoS attack, privacy leakages and VM manipulation attacks. MEC security is considered to be a top priority for the developers, as exploiting MEC may cause enormous amounts of damage. [22]

Solutions for both MCC and MEC have been proposed. In MCC, many of the proposals by standardization bodies, such as 3GPP, deal with the strategic use of different virtualization technologies, the dynamic allocation of data handling and the design and redesign of encryption methods. As VMs are used to connect to the virtual instances in the cloud, the security here is provided by isolating each user's virtual connection from others. For specifics threats, learning-based systems can be better than generic approaches. Learning-based systems take samples of packets, analyze them and learn certain attributes that are typical for malicious packets. This is a good solution to a DoS attack for example. As for the user's equipment, anti-malware ought to be installed to the devices or served from the cloud. As for application security, several different frameworks of implementations have been proposed, such as dynamic credential generation for identity protection, in-device spatial cloaking technology for privacy and overall frameworks produced by different cloud system providers. For MEC, there is less works that are made in terms of security. The usage of gateways in the networks at strategic points is recommended, such as IoT gateway. The applications that are hosted in the edges of the network should authenticate all the users attempting a connection. The MEC server itself should be configured in a way that protects the applications and data storage units from malicious activity. [22]

Signaling storm is an example of an attack that can be targeted at a cloud system. Mobile networks control plane is vulnerable to this type of attack. The attacks goal is to overload the control plane using traffic patterns, which causes the service to become extremely slow or unavailable. This differs from DoS attack, as DoS attack may target some other part of network, whereas signaling storm targets the control plane. Signaling storm may be caused by botnets or malware. Signaling storm can also be caused by mishap in developing an application. If a mobile application is designed in a way, that does not take into account the specifics of mobile networks, they may inadvertently cause a signaling overload. An example of this is the first release of Angry Birds on android devices, where the in-game advertisements caused excessive load due to frequent communication [26]. As said previously, these storms can be caused by a malware. Some examples in this

field are e-mail and SMS spammers, adware, botclients and premium service abusers. All the formerly mentioned generate small amounts of traffic, but they do it often. This requires repetitive allocation and deallocation of radio channels, which may lead to a negative impact in the control plane. [27]

One possible solution for signaling storms specifically is a software, that is installed in the signaling system or within the mobile devices. After repetitive high bandwidth requests are noticed, and the requests transfer no data or voice, the software would block the mobile device from trying to make another request. This not only defies the signaling storms, but also limits the energy consumption in the network and battery consumption of the mobile devices. [28]

6.1.4 Privacy problems and solutions in 5G

Privacy has been a talking point in previous technologies and continues to be one in 5G, as it is one of the subjects that everyone can chime in on. From the point of view of the users, the concerns arise from identity, data and location of your personal information. Many of the mobile phone applications these days require you to give them some sort of personal information before you can even download it. It is not often mentioned how and where the data is stored or for what purpose it is used. This gives users a veil of shadow and uncertainty considering their own personal information.

Attacks such as boundary attacks, timing attacks and semantic information attacks target the location section of the privacy. The location privacy can be leaked on the physical layer level because of the access point selection in 5G. If a malicious station is selected, the user's privacy is compromised. Attacks targeted at IMSI are threats as well. They aim to reveal the identity of the owner of the device that is targeted by this catching attack. For example, this type of attack can be carried out by using a fake base station which the user's device prefers if it has lost its TMSI. In this case, the device will send its IMSI to the fake base station, and IMSI contains the identity of the user. 5G networks also have a little bit of discrepancy between the different service provides, as the 5G networks have three different areas of providers. There are Communication Service Providers (CSPs), Virtual Mobile Network Operators (VMNOs) and network infrastructure providers. All these entities have different standards for their security policies, which can prove to be quite problematic. In the technologies leading up to 5G the mobile operators had full control of their system components. 5G mobile operators

are losing this full control of the privacy and security aspects, and therefore user privacy can be challenged where the same infrastructure is shared among different entities, such as VMNOs. Also, as there are no physical boundaries in the 5G networks as it uses NFV and cloud-based data storage, the different countries policies for data privacy might lead to users data being compromised as it is stored in the cloud in a different country. [22]

To preserve the user privacy, an agreement between users, service providers, application providers, network operators and many others, needs to be made when dealing with data usage and data storage. This requires transparency, openness and accountability from all sides. Mobile operators especially need to focus on having capabilities to store more sensitive data locally and less sensitive data in public clouds for example. Location privacy must be protected by using anonymity-based technologies where the users real identity should be replaced with pseudonyms. Encryption and location cloaking here are essential. For IMSI attacks specifically, TMSI should be used wherever applicable, as it is randomly generated by certain time intervals, and thus harder to track back to the user. The standardization process of making the 5G networks secure for users happens at three levels: Governmental level, where country and multi-national specific regulations are made, industry level, which includes certain standardization groups such as 3GPP and ETSI, and the consumer level, where the users themselves demand certain level of privacy. [22]

7 CONCLUSION

The goal of this thesis was to build an understanding of mobile wireless technologies that preceded 5G, and subsequently give an understanding of the new technologies coming with 5G and their security challenges. This thesis also discussed the privacy challenges coming with 5G. Potential solutions are presented in this thesis for the NFV, SND, cloud computing and MEC technologies as well as privacy. The information used in this thesis consisted mainly of research papers on the subject.

This thesis provides a basic knowledge of technologies preceding 5G and their security features. This thesis gives information about the new technologies coming with 5G, and their security challenges and potential solutions. This research should also give some level of understanding of who is in charge of the implementation and what sort of hierarchy exists in terms of standardizing network security.

These challenges mainly concern customers and other 5G service buyers, as they are the ones that actually suffer the consequences if vulnerabilities are not found out before they are exploited. Therefore, mobile operators must be held to a high standard by their service users, so they do not economize on security features.

The future of 5G is what is exciting. In the upcoming years it will be deployed in cities and perhaps even in dense urban areas. As this technology is rolled out, more research needs to be carried out as vulnerabilities are found. As the use cases for 5G are many, a good research topic for the future could be the level of security needed for each IoT device, as IoT related technology is starting to escalate.

REFERENCES

1. Liyanage, M., Ahmad, I., Abro, AB., Gurtov, A., Ylianttila, M. A comprehensive guide to 5G security [Internet]. New Jersey: John Wiley & Sons; 2018 [cited 2020 Mar 27]. 441 p. Available from: https://ebookcentral.proquest.com/lib/turkuamk-ebooks/detail.action?docID=5216619

2. Mohammad, MM., Kumar, S. Evolution of Mobile Wireless Technology from 0G to 5G [Internet]. 2015 [cited 2020 Mar 27];6(3):1-7. Available from https://ijcsit.com/docs/Volume%206/vol6issue03/ijcsit20150603123.pdf

3. Kovaleva, M. Global 2G and 3G Phase Out/Sunset: What Do We Know So Far? [Internet]. [place unknown]: Emnify. 2019 May [cited 2020 Mar 30] Available from: https://www.emnify.com/blog/global-2g-phase-out

4. Pannu, M., Bird, R., Gill, B., Patel K. Investigating vulnerabilities in GSM security. In: IEMCON 2015 [Internet]; 2015 Oct; University of British Columbia, Canada. Vancouver: Researchgate; 2015 Oct [cited 2020 Mar 31]; p. 1-6. Available from: https://www.researchgate.net/publication/283723257_Investigating_Vulnerabilities_in_GSM_Security

5. Toorani, M., Beheshti, A. Solutions to the GSM security weaknesses. In: NGMAST'08 [Internet]; 2008 Sep; United Kingdom. [place unknown]: Researchgate; 2008 Sep [cited 2020 Apr 2]; p. 1-6. Available from: https://www.researchgate.net/publication/45901514_Solutions_to_the_GSM_Security_Weaknesses

6 3GPP. Specification numbering [Internet]. [place unknown]: 3GPP; 2020 [updated 2019 Jan 12; cited 2020 Apr 5]. Available from: https://www.3gpp.org/specifications/specification-numbering

7 Ertaul, L., Natte, S., Saldalmi, G. In: ICWN 2010 [Internet]. 2010 Jul 12-15; Las Vegas, USA. Nevada: Researchgate; 2010 Jan [cited 2020 Apr 5]; p. 1-7. Available from: https://www.researchgate.net/publication/220719254_Security_Evaluation_of_CDMA2000

8 Thomson, I. After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts [Internet]. San Francisco: The Register; 2017 May 3 [cited 2020 Apr 5]. Available from: https://www.theregister.co.uk/2017/05/03/hackers_fire_up_ss7_flaw/

9 Positive Technologies. SS7 network security analysis report [Internet]. [place unknown]: Positive Technologies; 2020 Feb 18 [cited 2020 Apr 5]. Available from: https://positive-tech.com/research/ss7-network-security-analysis-2020/

10 Ericsson. World's first 4G/LTE network goes live today in Stockholm [Internet]. [place unknown]: Ericsson; 2009 [updated 2009 Dec 14; cited 2020 Apr 5]. Available from: https://www.ericsson.com/en/press-releases/2009/12/worlds-first-4glte-network-goes-live-today-in-stockholm

11 Jowitt, T. Tales in Tech History: WiMax [Internet]. [place unknown]: Silicon UK; 2018 [updated 2018 Feb 2; cited 2020 Apr 10]. Available from: https://www.silicon.co.uk/networks/tales-tech-history-wimax-227889

12 Iwamura, M., Takahashi, H., Nagata, S. Relay technology in LTE-Advanced. NTT DOCOMO Technical journal [Internet]. 2010 Sep [cited 2020 Apr 8];12(2):29-36. Available from: https://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/rd/technical_journal/bn/vol12_2/vol12_2_029en.pdf

13 Netmanias. LTE Security I: Concept and authentication [Internet]. [place unknown]: Netmanias; 2013 Jul 31 [cited 2020 Apr 11]. Available from: https://www.netmanias.com/en/?m=view&id=techdocs&no=10425

14 Ahmed, MS. A Stude on IEEE 802.16 (WiMAX) and its security issues [Internet]. [place unknown]: IJATER; 2014 Mar [cited 2020 Apr 11]. Available from: https://www.researchgate.net/publication/303280264_A_STUDY_ON_IEEE_80216_WIMAX_AND_ITS_SECURITY_ISSUES

15 Piqueras Jover, R. LTE security, protocol exploits and location tracking experimentation with low-cost software radio [Internet]. New York: Bloomberg LP; 2016 Jul 18 [cited 2020 Apr 12]. Available from: https://www.researchgate.net/publication/305401180_LTE_security_protocol_exploits_and_location_tracking_experimentation_with_low-cost_software_radio

16 Ericsson. This is 5G [Internet]. Stockholm, Sweden: Ericsson; 2018 [cited 2020 Apr 13]. Available from: https://www.ericsson.com/4a3114/assets/local/newsroom/media-kits/5g/doc/ericsson_this-is-5g_pdf_v4.pdf

17 GSMA. The Mobile Economy [Internet]. MWC Barcelona: GSMA; 2020 [cited 2020 Apr 13]. Available from: https://www.gsma.com/mobileeconomy/

18 ETSI. Comparison of key capabilities of IMT-Advanced with IMT-2020 [Image on internet]. [place unknown]: ETSI; 2018 [cited 2020 Apr 17]. Available from: https://www.etsi.org/technologies/5g

19 Cooney, M. What is SDN and where software-defined networking is going [Internet]. Framingham, MA: Networkworld; 2019 [cited 2020 Apr 17]. Available from: https://www.networkworld.com/article/3209131/what-sdn-is-and-where-its-going.html

20 Elisa. Kuuluvuuskartta [Internet]. [place unknown]: Elisa; 2020 [cited 2020 Apr 19]. Available from: https://elisa.fi/kuuluvuus/

21 NGMN. 5G white paper [Internet]. Frankfurt, Germany: NGMN; 2015 [cited 2020 Apr 21]. Available from: https://www.ngmn.org/work-programme/5g-white-paper.html

22 Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., Gurtov, A. Overview of 5G security challenges and solutions. IEEE communications standards magazine [Internet]. 2019 Feb 12 [cited 2020 Apr 21];2(1):36-43. Available from: http://jultika.oulu.fi/Record/nbnfi-fe201902124647

23 Martin, AB., Marinos, L., Rekleitis, E., Spanoudakis, G., Petroulakis, N. Threat Landscape and Good Practice Guide for Software Defined Networks/5G [Internet]. Heraklion, Greece: ENISA; 2016 Jan 27 [cited 2020 Apr 23]. 72 p. Available from: https://www.enisa.europa.eu/publications/sdn-threat-landscape
doi: 10.2824/67261

24 Alwakeel, AM., Alnaim, A., Fernández, EB. A Survey of Network Function Virtualization Security. In: IEEE SoutheastCon 2018 [Internet]; 2018 Apr 19-22; St. Petersburg, Florida, USA. Boca Raton: Florida Atlantic University; 2018 [cited 2020 Apr 24]; p. 1-7. Available from: https://www.researchgate.net/publication/328146655_A_Survey_of_Network_Function_Virtualization_Security

25 Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., Gurtov, A. 5G Security: Analysis of Threats and Solutions: 2017 IEEE Conference on Standards for Communications and Networking [Internet]; 2017 Sep 18-20; Helsinki, Finland. Helsinki: IEEE; 2018 Jul 30 [cited 2020 Apr 26]; p. 193-199. Available from: http://jultika.oulu.fi/Record/nbnfi-fe2018073033104

26 IT Wire. Angry Birds + Android + ads = network overload [Internet]. [place unknown]: IT Wire; 2011 Jun 14 [cited 2020 Apr 28]. Available from: https://www.itwire.com/business-it-news/networking/47823-angry-birds-android-ads-network-overload

27 Gorbil, G., Abdelrahman, OH., Pavloski, M., Gelenbe, E. Storms in Mobile Networks. In: MSWiM'14 [Internet]; 2014 Sep; Montreal QC Canada. New York, USA: Association for Computing Machinery; 2014 Nov 5 [cited 2020 Apr 29]; p. 119-126. Available from: https://arxiv.org/pdf/1411.1280.pdf

28 Gelenbe, E., Abdelrahman, OH., Gorbil, G. Detection and Mitigation of Signalin Storms in Mobile Networks. In: 2016 ICNC [Internet]; 2016 Feb 15-18; Kauai, Hawaii, USA. London, England: Intelligent Systems and Networks Group; 2016 [cited 2020 Apr 30]; p. 1-5. Available from: https://www.researchgate.net/publication/301610953_Detection_and_mitigation_of_signaling_storms_in_mobile_networks